Abstract of the Disclosure

Cryptographic systems and methods that support multiple modes of operation, such as CBC, CTR and/or CCM modes. In one aspect, a method for encrypting data includes reading a plaintext data block from a memory, storing the plaintext data block in an input buffer, encrypting the plaintext data block in the input buffer using a first mode to generate a first ciphertext, storing the first ciphertext in an output buffer, encrypting the plaintext data block in the input buffer using a second mode to generate a second ciphertext. For example, in a CCM mode of operation wherein the first mode is a CTR (counter) mode and the second mode is a CBC (cipher block chaining) mode, the block of plaintext that is initially read from memory and stored in the data input register is applied to both the CTR and CBC modes, thereby reducing a number memory read operations as in conventional CCM modes.